REMARKS

Applicants respectfully request favorable reconsideration of this application, as amended.

Applicants acknowledge with appreciation the Examiner's renumbering of the Claims 19-38.

By this Amendment, the claims have been amended for clarity of expression, consistency, and conformance with U.S. practice. Claims 19, 33 and 39 have also been amended as discussed in detail below. Claims 37 and 38 have been canceled without prejudice or disclaimer to reduce the issues, and Claims 39 and 40 have been added. Claims 1-18 were previously canceled without prejudice or disclaimer. Thus, Claims 19-36, 39 and 40 are pending.

In the Office Action, Claims 19-31 were rejected under 35 U.S.C. § 101 as allegedly being directed to non-statutory subject matter; and Claims 19-38 were rejected under 35 U.S.C. § 102(b) over U.S. Patent No. 6,161,183 to Saito et al. ("Saito").

Without acceding to the rejection under 35 U.S.C. § 101, Claim 19 has been amended to recite, *inter alia*, a group signature device including means for producing a group signature (S) using a message (m) and personalized data (z, Kz) such that a checker, upon receiving the message (m) accompanied by the group signature (S), is able to verify that the message (m) is associated with a group (G) based on the personalized data (z, Kz) and the group signature (S), to authenticate the message (m) with the identity of the member (M) of the group (G) remaining anonymous to the checker; and means for outputting the message (m) and the group signature (S) to the checker. Support is provided, for example, at page 10, lines 9-23; page 12, lines 8-14; page 14, lines 5-7; page 15, lines 25-27; page 17, lines 14-21; and FIGs. 3 and 4 of Applicants' disclosure.

Therefore, Applicant respectfully submits that Claim 19 clearly recites a useful, concrete and tangible result having a practical application; for example, producing and outputting a group signature to authenticate a message with the identity of the member of the group remaining anonymous. See *State Street Bank & Trust Co. v. Signature Financial Group Inc.*, 149 F.3d 1368, 1373-75 (Fed. Cir. 1998).

Furthermore, Claim 33 has been amended to recite, *inter alia*, a method for secure communication including producing a group signature (S) of a message (m) with a private key (SK) common to members (M) of a group (G), outputting the message (m) along with the group signature (S), and verifying that the message (m) is associated with the group (G) based on the personalized data (z, Kz) and the group signature (S) to authenticate the message (m) without identifying the member (M) of the group (G).

In addition, Claim 39 has been amended to recite, *inter alia*, a group signature system for authenticating a message (m) accompanied by a group signature (S), including an electronic device configured to. . . produce the group signature (S) using the message (m) and personalized data (z, Kz), and to output the message (m) and the group signature (S), and a checker that receives the message (m) accompanied by the group signature (S) output from the electronic device and being configured to verify that the message (m) is associated with the group (G) based on the personalized data (z, Kz) and the group signature (S), the identity of the member (M) remaining anonymous to the checker.

Therefore, Applicants respectfully submits that Claims 33 and 39 also clearly recite a useful, concrete and tangible result having a practical application, for at least the same reasons discussed above with respect to Claim 19.

Applicants respectfully request that the rejection under 35 U.S.C. § 101 be withdrawn.

Without acceding to the rejection under 35 U.S.C. § 102(b), Claim 19 recites, *inter alia*, a group signature device including means for producing a group signature (S) using a message (m) and personalized data (z, Kz) such that a checker, upon receiving the message (m) accompanied by the group signature (S), is able to verify that the message (m) is associated with a group (G) based on the personalized data (z, Kz) and the group signature (S), to authenticate the message (m) with the identity of the member (M) of the group (G) remaining anonymous to the checker. It is apparent that the applied reference does not teach or suggest at least these features of Claim 19.

For example, Saito teaches a data verifying apparatus and method in which a message is accompanied by a digital signature using a private key associated with a particular person. *See* Saito, col. 7, lines 35-42 and 52-53. Saito does not appear to teach or suggest producing a group signature to verify a message based on the group signature with the identity of the member of the group remaining anonymous, as recited in Claim 19.

Therefore, Applicants respectfully submit that Claim 19 distinguishes patentably from Saito.

Independent Claim 33 recites, *inter alia*, a method for secure communication including producing a group signature (S) of a message (m) with a private key (SK) common to members (M) of a group (G), and verifying that the message (m) is associated with the group (G) based on the personalized data (z, Kz) and the group signature (S) to authenticate the message (m) without identifying the member (M) of the group (G).

In addition, independent Claim 39 recites, *inter alia*, a group signature system for authenticating a message (m) accompanied by a group signature (S), including an electronic device configured to. . . produce the group signature (S) using the message (m)

and personalized data (z, Kz), and a checker configured to verify that the message (m) is associated with the group (G) based on the personalized data (z, Kz) and the group signature (S), the identity of the member (M) remaining anonymous to the checker.

Therefore, Applicants respectfully submits that Claims 33 and 39 also distinguish patentably from Saito for at least the reasons discussed above with respect to Claim 19.

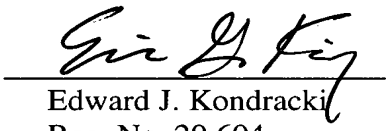
The remaining Claims 20-32, 34-36 and 40 are also believed to distinguish patentably due to their respective dependence from Claims 19, 33 and 39, as well as for the additional features recited in Claims 20-32, 34-36 and 40. Support for Claims 20-32, 34-36 and 40 is additionally provided, for example, at page 16, line 27 to page 17, line 6; page 17, lines 3-13; page 19, lines 5-28; page 20, lines 1-8; page 22, lines 12-21; page 23, lines 11-21; and FIGs. 5-7.

Applicants respectfully submit that this application is in condition for allowance. A prompt Notice of Allowance is respectfully requested.

The Commissioner is hereby authorized to charge to Deposit Account No. 50-1165 (T2151-9156US01) any fees under 37 C.F.R. §§ 1.16 and 1.17 that may be required by this paper and to credit any overpayment to that Account. If any extension of time is required in connection with the filing of this paper and has not been separately requested, such extension is hereby requested.

Respectfully submitted,

Date: September 4, 2007

By: 

Edward J. Kondracki
Reg. No. 20,604

Eric G. King
Reg. No. 42,736

Miles & Stockbridge, P.C.
1751 Pinnacle Drive
Suite 500
McLean, Virginia 22102-3833
(703) 903-9000

4814-8400-4353